CLAIMS

What is Claimed Is:

1. A method for controlling access to a network, the method comprising the following steps:

(a) coupling a user device to a network;

(b) transmitting a first response to the network;

(c) generating a second response upon receipt of the first response by the network;

(d) comparing the first response and second response; and

(e) authenticating the user device if the first response and second response match, and not authenticating the user device if the first response and second do not match.

2. The method of Claim 1 wherein the first response includes a public shared secret.

3. The method of Claim 1 wherein the first response includes a private shared secret.

4. The method of Claim 1 wherein the first response includes a public shared secret and a private shared secret.

5. The method of Claim 1 wherein the second response includes a public shared secret.

6. The method of Claim 1 wherein the second response includes a private shared secret.

7. The method of Claim 1 wherein the second response is generated by the network.

8. A method for controlling access to a network, the method comprising the following steps:

(a) coupling a user device to a network;

(b) transmitting a request to the network;

(c) transmitting a challenge to the user device;

(d) generating a first response;

(e) transmitting the first response to the network;

(f) generating a second response upon receipt of the first response by the network;

(g) comparing the first response and second response; and

(h) authenticating the user device if the first response and second response match, and not authenticating the user device if the first response and second do not match.

9. The method of Claim 8 wherein the first response includes a symmetric public shared secret.

10. The method of Claim 8 wherein the first response includes a symmetric private shared secret.

11. The method of Claim 8 wherein the first response includes a symmetric public shared secret and a symmetric private shared secret.

12. The method of Claim 8 wherein the second response includes a symmetric public shared secret.

13. The method of Claim 8 wherein the second response includes a symmetric private shared secret.

14. The method of Claim 8 wherein the second response is generated by the network.

15. A method for controlling access to a public network, the method comprising the following steps:

(a) coupling a user device to a public network, the network including a server;

(b) transmitting an access request from the user device to the server;

(c) transmitting a challenge from the server to the user device;

(d) processing the challenge to ascertain a selected public shared secret stored on the user device;

(e) generating a first response using at least the selected public shared secret;

(f) transmitting the first response to the server;

(g) generating a second response upon receipt of the first response by the server;

(h) comparing the first response and second response; and

(i) authenticating the user device to grant access to the public network if the first response and second response match, and not authenticating the user device if the first response and second do not match.

16. The method of Claim 15 wherein the first response includes a symmetric public shared secret.

17. The method of Claim 15 wherein the second response includes a symmetric public shared secret.

18. The method of Claim 8 wherein the second response is generated by the server.

19. A method for controlling access to a private network, the method comprising the following steps:

(a) coupling a user device to a private network, the network including a server;

(b) transmitting an access request from the user device to the server;

(c) transmitting a challenge from the server to the user device;

(d) processing the challenge to ascertain at least a selected private shared secret stored on the user device;

(e) generating a first response using at least the selected private shared secret;

(g) transmitting the first response to the server;

(h) generating a second response upon receipt of the first response by the server;

(i) comparing the first response and second response; and

(j) authenticating the user device to grant access to the private network if the first response and second response match, and not authenticating the user device if the first response and second do not match.

20. A method for controlling access to a private network, the method comprising the following steps:

(a) coupling a user device to a private network, the network including an access control server;

(b) transmitting an access request from the user device to the server, the access request comprising a first response that includes a selected public shared secret and a selected private shared secret stored on the user device;

(c) invoking the server to generate a second response upon receipt of the first response, the server generating the second response by means of the following steps,

(i) processing the challenge transmitted to the user device to retrieve the selected public shared secret and the selected private shared secret, and

(ii) processing the selected public shared secret and selected private shared secret to generate the second response;

(h) comparing the first response and second response; and

(i) authenticating the user device to grant access to the private network if the first response and second response match, and not authenticating the user device if the first response and second do not match.

21. The method of Claim 20 wherein the first response includes a symmetric public shared secret and a symmetric private shared secret.

22. The method of Claim 20 wherein the second response includes a symmetric public shared secret and a symmetric private shared secret.

23. A method for controlling access to a private network, the method comprising the following steps:

(a) coupling a user device to a private network, the network including an access control server;

(b) transmitting an access request from the user device to the server;

(c) transmitting a challenge from the server to the user device;

(d) processing the challenge to retrieve a selected public shared secret and a selected private shared secret stored on the user device;

(e) processing the selected public shared secret and selected private shared secret to generate a first response;

(f) transmitting the first response to the server;

(g) invoking the server to generate a second response upon receipt of the first response by the server, the server generating the second response by means of the following steps,

(i) processing the challenge transmitted to the user device to retrieve the selected public shared secret and the selected private shared secret, and

(ii) processing the selected public shared secret and selected private shared secret to generate the second response;

(h) comparing the first response and second response; and

(i) authenticating the user device to grant access to the private network if the first response and second response match, and not authenticating the user device if the first response and second do not match.